PassQueen
a.k.a dumpsqueen.com

Certified Secure Software Lifecycle Professional

ISC2 CSSLP

Version Demo

Total Demo Questions: 46

Total Premium Questions: 464

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Secure Software Concepts	157
Topic 2, Secure Software Requirements	13
Topic 3, Secure Software Architecture and Design	28
Topic 4, Secure Software Implementation	24
Topic 5, Secure Software Testing	51
Topic 6, Secure Software Lifecycle Management	95
Topic 7, Secure Software Deployment, Operations, Maintenance and Disposal	88
Topic 8, Mix Questions	8
Total	464

QUESTION NO: 1

Which of the following is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.

B. A CI that particularly refers to a software version.

C. A CI that has the same essential functionality as another CI but a bit different in some small manner.

D. A CI that particularly refers to a hardware specification.

ANSWER: C

Explanation:

A CI that has the same essential functionality as another CI but a bit different in some small manner is a variant because it represents a controlled configuration-item instance that belongs to the same functional family as another item while retaining a meaningful, documented difference. The difference may concern a platform, build, component selection, supported interface, capacity, or another approved attribute, but it does not alter the item's core intended purpose. Configuration management must identify and record such distinctions so that teams can establish accurate baselines, understand dependencies, reproduce a deployed configuration, and assess the impact of a change on all related items. Treating variants as identifiable CIs or CI forms also supports traceability: a team can determine which specific implementation was tested, approved, released, and is operating in an environment. This is particularly important in secure software lifecycle work, where a seemingly small variation—such as a library build, operating-system target, or enabled security feature—can affect security posture and change-control decisions. NIST describes configuration management as maintaining the integrity of systems through processes for identifying and controlling configuration items and changes; see NIST SP 800-128, Guide for Security-Focused Configuration Management. Related configuration-management terminology is also available in the ISO/IEC/IEEE 24765 systems and software engineering vocabulary.

QUESTION NO: 2

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.

A. Testing

B. Implementation

C. Operation/maintenance

D. Development/acquisition

E. Disposal

F. Initiation

ANSWER: B C D E F

Explanation:

Implementation, Operation/maintenance, Development/acquisition, Disposal, and Initiation are the lifecycle phases in the generic system development lifecycle model used in United States government security guidance. Initiation establishes the business need, scope, preliminary risk considerations, and high-level security requirements before a solution is selected or built. Development/acquisition covers obtaining or creating the system and integrating security requirements and controls throughout that work. Implementation places the system into its operational environment, including validation, authorization-related activities, deployment, and user readiness. Operation/maintenance is the continuing phase in which the system is run, monitored, patched, changed, and maintained while security risks are managed. Disposal addresses the secure retirement of the system, including retention or destruction of information, sanitization of media, archival needs, and orderly replacement or decommissioning. NIST identifies these phases as initiation; development/acquisition; implementation; operations/maintenance; and disposition. "Disposal" is a commonly used equivalent for disposition in lifecycle descriptions,

so it represents the same end-of-life phase in this question. See NIST's Security Considerations in the System Development Life Cycle and the NIST glossary definition of system development life cycle.

QUESTION NO: 3

Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.

A. Data classification

ANSWER: A

Explanation:

Data classification is the appropriate phrase because it assigns data a category according to its sensitivity, confidentiality impact, business value, and handling needs. That category drives the protections required throughout the data lifecycle—not merely while data is stored, but also while it is processed and transferred. For example, a classification policy can require access restrictions, encryption, approved processing environments, retention requirements, secure transmission methods, and labeling for data designated as sensitive. Classification also gives system owners and development teams a consistent basis for selecting controls proportionate to the consequences of unauthorized disclosure, modification, or loss. In secure software lifecycle work, this is important because software requirements, architecture, test cases, and operational procedures must protect information according to its assigned classification. NIST describes categorization as establishing the security impact level needed to select appropriate safeguards, while NIST control guidance includes protections for information in storage and in transit. See NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories and NIST SP 800-53 Rev. 5.

QUESTION NO: 4

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

A. SNMP enumeration

B. IIS buffer overflow

C. NetBIOS NULL session

D. DNS zone transfer

E. IIS Internet Printing Protocol (IPP) buffer overflow

ANSWER: B E

Explanation:

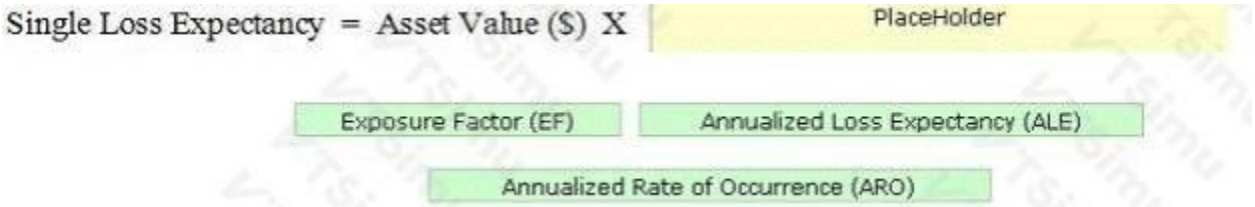
"IIS buffer overflow" is correct because Internet Printing Protocol functionality in affected versions of Microsoft Internet Information Services was implemented through the Internet Printing ISAPI extension. Microsoft documented a vulnerability in that extension in which a malformed HTTP request could overrun a buffer, potentially allowing an attacker to execute code in the security context of the IIS service. Removing or disabling the IPP printing capability eliminates the vulnerable Internet Printing component when that service is not required, thereby reducing the server's attack surface. "IIS Internet Printing Protocol (IPP) buffer overflow" is also correct because it states the same vulnerability more precisely: the relevant buffer-overflow exposure is specifically associated with IIS Internet Printing support, rather than with an unrelated server feature. This is a sound secure-operations practice: disable unnecessary services and extensions, then apply vendor security updates to components that must remain enabled. Microsoft's bulletin describes the Internet Printing ISAPI extension buffer-overrun issue and lists removal or disabling of the extension as a mitigation for systems that do not need Internet printing. See Microsoft Security Bulletin MS01-023 and Microsoft IIS features documentation.

QUESTION NO: 5 - (DRAG DROP)

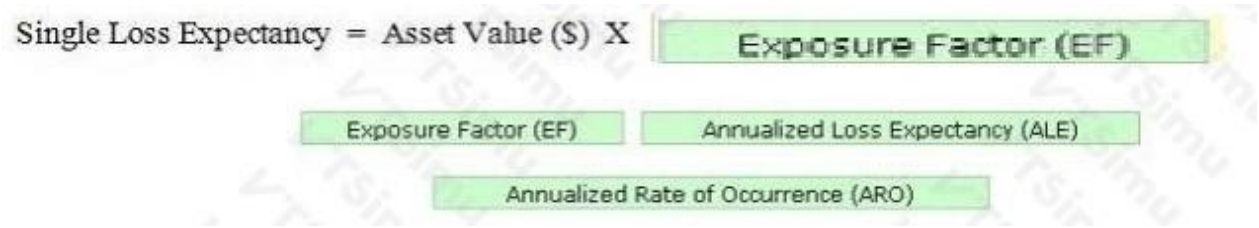
DRAG DROP

Drop the appropriate value to complete the formula.

Select and Place:



ANSWER:



Explanation:

Single Loss Expectancy is calculated by multiplying the value of the asset by the Exposure Factor: SLE = Asset Value × Exposure Factor. The Exposure Factor expresses the portion, usually represented as a percentage, of the asset's value that would be lost if a particular threat event occurs once. For example, if an asset is valued at $100,000 and the expected damage from one occurrence is 25 percent, the Exposure Factor is 0.25 and the Single Loss Expectancy is $25,000. This makes Exposure Factor the value required to complete the displayed formula.

This relationship is a core part of quantitative risk analysis. It converts an estimate of impact into a monetary loss for one occurrence, enabling an organization to compare potential risks consistently and make informed decisions about safeguards, risk treatment, and spending. Once Single Loss Expectancy has been determined, it can be combined with the estimated yearly frequency of the event to calculate Annualized Loss Expectancy, which represents expected loss over a year. The formula shown, however, is specifically for the loss from one event, so it correctly uses Asset Value and Exposure Factor. ISC2's overview of risk management concepts is available through the ISC2 CISSP Student Guide, and NIST discusses applying impact and likelihood in risk assessment in NIST SP 800-30 Rev. 1.

QUESTION NO: 6

Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?

A. Information Systems Security Officer (ISSO)

B. Designated Approving Authority (DAA)

C. System Owner

D. Chief Information Security Officer (CISO)

E. Authorizing Official (AO)

ANSWER: B E

Explanation:

The **Designated Approving Authority (DAA)**, now more commonly called the **Authorizing Official (AO)**, is accountable for the authorization decision for an information system. This decision includes determining whether the system's remaining, or residual, risk is acceptable for organizational operation. The AO is a senior official with the authority to commit organizational resources and explicitly accept responsibility for operating the system despite known risk. This role is central to the NIST Risk Management Framework authorization step, where the AO reviews the security and privacy assessment results, plans of action and milestones, and the system's risk posture before authorizing operation, authorizing operation with conditions, or declining authorization. "Designated Approving Authority" is the legacy term used in earlier certification-and-accreditation processes; it represents the same risk-acceptance authority as the modern Authorizing Official. Therefore, both terms correctly identify the official who accepts or rejects residual system risk. NIST defines the Authorizing Official and describes this authorization responsibility in its Authorizing Official glossary entry and in SP 800-37 Rev. 2, Risk Management Framework.

QUESTION NO: 7

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

A. Reliability test

B. Performance test

C. Regression test

D. Functional test

ANSWER: B

Explanation:

Performance test is correct because performance testing evaluates how a build behaves under defined workload conditions and establishes measurable operational limits. A team can use it to determine response times, throughput, resource consumption, scalability, and behavior as concurrency or transaction volume increases. These results identify the point at which the build no longer meets agreed performance criteria, such as a maximum acceptable response time or minimum transactions-per-second target. That point represents a practical performance threshold for the build and provides objective evidence for release decisions, capacity planning, and remediation of bottlenecks.

Within a secure software lifecycle, performance testing should be repeatable and based on documented workloads, environments, metrics, and acceptance criteria. Testing successive builds also lets engineers detect degradation introduced by code, configuration, dependencies, or infrastructure changes. The ISC2 CSSLP examination outline includes security testing and assessment activities across the software lifecycle, while performance engineering supports the dependable operation of software in its intended environment. The ISTQB glossary definition of performance testing describes testing that determines responsiveness, throughput, utilization, and related quality characteristics under specified conditions. NIST also discusses performance and capacity considerations in its Systems Security Engineering publication.

QUESTION NO: 8

"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

A. Leverage attack patterns

B. Compiler security checking and enforcement

C. Tools to detect memory violations

D. Safe software libraries

E. Code for reuse and maintainability

ANSWER: B C D

Explanation:

Compiler security checking and enforcement, **tools to detect memory violations**, and **safe software libraries** are tools and practices specifically identified in *Enhancing the Development Life Cycle to Produce Secure Software*. Compiler-based checking and enforcement can identify or prevent unsafe constructs during compilation and can enable protective compiler features. Memory-violation detection tools help uncover defects such as invalid memory accesses, buffer overflows, and memory-management errors that could otherwise become exploitable vulnerabilities. Safe software libraries provide implementations designed to reduce the likelihood of common programming errors and give developers safer interfaces for security-sensitive operations.

These measures support secure software development by building security-relevant checks and safer implementation choices into the engineering workflow, rather than relying solely on post-release discovery. They also align with modern secure-development guidance: the NIST Secure Software Development Framework calls for practices that prevent, identify, and mitigate vulnerabilities throughout software development and maintenance. See the original DHS report at DHS: Enhancing the Development Life Cycle to Produce Secure Software and the NIST SP 800-218 Secure Software Development Framework.

QUESTION NO: 9

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.

B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.

C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.

D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

ANSWER: D

Explanation:

Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It builds on qualitative risk analysis, which initially evaluates and prioritizes risks using relative characteristics such as probability and impact. The quantitative process then applies numerical methods and objective data, where available, to determine the aggregate effect of uncertainty on objectives such as cost, schedule, and performance. Common techniques include expected monetary value analysis, decision-tree analysis, sensitivity analysis, and Monte Carlo simulation. Its purpose is to support better-informed decisions by expressing potential risk exposure in measurable terms, such as a range of possible completion dates, the probability of meeting a budget target, or an estimated contingency reserve. Quantitative analysis is generally focused on the risks that have been identified and prioritized as significant enough to warrant further analysis. This definition aligns with established project-risk-management terminology and accurately distinguishes numerical analysis of overall objective exposure from the initial relative prioritization of risks. See the Project Management Institute's PMBOK Guide resources and the PMI overview of quantitative risk-analysis techniques.

QUESTION NO: 10

Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Role-Based Access Control

B. Discretionary Access Control

C. Policy Access Control

D. Mandatory Access Control

ANSWER: A D

Explanation:

Mandatory Access Control is the primary model described by the question. In MAC, a central authority defines and enforces access rules rather than allowing an individual resource owner to change permissions at will. System objects are assigned security labels, such as Confidential or Secret, and subjects receive clearances or authorizations. The system evaluates those centrally defined attributes and rules before permitting access. This creates a predetermined, consistently enforced access structure for protected objects and is especially appropriate where information classification and strong control of data flow are required.

Role-Based Access Control also uses predefined privileges, although it organizes them through roles. Administrators define permissions to system objects and associate those permissions with organizational roles; users receive access by being assigned the appropriate role. Consequently, the access privileges applicable to an object can be predefined and centrally administered rather than individually determined for each user. This model supports consistent enforcement of least privilege and separation of duties as personnel move between job functions. The CSSLP examination outline includes access-control concepts within secure software requirements and design considerations; see the ISC2 CSSLP Exam Outline. NIST also describes RBAC as associating permissions with roles and assigning users to those roles in its Role-Based Access Control project.

QUESTION NO: 11

You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.

B. It is a risk that can not be addressed by a risk response.

C. It is a risk that will remain no matter what type of risk response is offered.

D. It is a risk that remains after planned risk responses are taken.

ANSWER: D

Explanation:

It is a risk that remains after planned risk responses are taken. Residual risk is the exposure that continues to exist after an organization has selected and implemented risk treatment measures, such as mitigating controls, process changes, contractual transfers, or other planned responses. A response can reduce either the likelihood of an adverse event, its impact, or both, but it rarely reduces risk to absolute zero. For example, secure coding practices, peer review, testing, and runtime protections can substantially reduce the probability and impact of a software vulnerability, while some remaining exposure may still need to be monitored and accepted by the appropriate risk owner.

This concept is important in a secure software lifecycle because security decisions must account for what remains after safeguards are operating, rather than treating implementation of a control as proof that the risk has disappeared. The residual level should be evaluated against the organization’s risk tolerance and documented so that stakeholders can decide whether further treatment is justified or formal acceptance is appropriate. NIST defines residual risk as the risk remaining after security controls have been applied, and its risk-management guidance treats control selection and ongoing monitoring as part of managing that remaining exposure. See the NIST CSRC definition of residual risk and NIST SP 800-37 Rev. 2.

QUESTION NO: 12

The NIST ITL Cloud Research Team defines some primary and secondary technologies as the fundamental elements of cloud computing in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation. Which of the following technologies are included in the primary technologies? Each correct answer represents a complete solution. Choose all that apply.

A. Web application framework

B. Free and open source software

C. SOA

D. Virtualization

ANSWER: B C D

Explanation:

Free and open source software, SOA, and Virtualization are included among the primary technologies identified in the NIST ITL Cloud Research Team's cloud-computing technology taxonomy. Virtualization is foundational because it abstracts and pools physical compute, storage, and networking resources, enabling the elastic provisioning and tenant isolation associated with cloud services. SOA supports the composition and delivery of interoperable services through well-defined interfaces, a model that aligns with cloud-based service delivery. Free and open source software is also identified as a primary enabling technology because widely available, modifiable software platforms and components have supported the scalable infrastructure and service ecosystems used in cloud environments. These technologies complement the essential cloud characteristics described by NIST, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. NIST's authoritative cloud-computing definition and terminology are available in NIST Special Publication 800-145. Additional NIST cloud-computing resources, including program materials and guidance, are available through the NIST Cloud Computing Program.

QUESTION NO: 13

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution. Choose all that apply.

A. Moderate

B. Medium

C. High

D. Low

ANSWER: B C D

Explanation:

FIPS 199 defines three potential impact levels for security categorization of federal information and information systems: **Low**, **Medium**, and **High**. These levels are assigned by considering the potential adverse effect that a loss of confidentiality, integrity, or availability could have on an organization, its operations and assets, or individuals. A low impact represents a limited adverse effect; a medium impact represents a serious adverse effect; and a high impact represents a severe or catastrophic adverse effect. The categorization is a foundational risk-management activity because it informs the selection and tailoring of security controls and helps ensure that protections are proportionate to the sensitivity and criticality of the information system. FIPS 199 specifies that a system security category considers each security objective—confidentiality, integrity, and availability—and uses the highest applicable impact value when determining the system-level category. Therefore, the defined potential-impact values are **Medium**, **High**, and **Low**. The authoritative definitions appear in NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. Additional implementation guidance is provided in NIST SP 800-60 Volume I.

QUESTION NO: 14

Which of the following are examples of passive attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Dumpster diving

B. Placing a backdoor

C. Eavesdropping

D. Shoulder surfing

ANSWER: A C D

Explanation:

Passive attacks obtain information without changing system data, processing, configurations, or service operation. **Dumpster diving** is passive because an attacker searches discarded documents, storage media, labels, or other materials to recover sensitive information while leaving the target system itself untouched. **Eavesdropping** is passive when an attacker listens to or captures communications in order to learn their contents, traffic patterns, credentials, or other sensitive data without altering the communication. **Shoulder surfing** is also passive because the attacker observes a user's screen, keyboard input, printed materials, or work area to collect information without interacting with or modifying the system. These activities primarily compromise confidentiality, which is the characteristic impact associated with passive information-gathering attacks. Secure software and organizational security practices should account for such threats through measures such as encryption for communications, careful media-disposal procedures, screen privacy controls, and user awareness training. NIST describes passive attacks as attacks that monitor or observe communications or information without modifying resources; see NIST SP 800-12 Rev. 1. The broader security objective of protecting information from unauthorized disclosure is also addressed in FIPS 200.

QUESTION NO: 15

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System

B. Integrated Change Control

C. Configuration Management System

D. Scope Verification

ANSWER: C

Explanation:

The Configuration Management System is the component that provides the disciplined control needed to evaluate, test, record, and track changes affecting defined project items, including scope-related deliverables and their associated documentation. Configuration management establishes identifiable baselines and maintains the status and version history of configuration items. When a proposed scope change is approved through the applicable change-control process, the Configuration Management System ensures that the affected artifacts can be assessed against the established baseline, updated in a controlled manner, tested or verified as required, and documented so the project team has an authoritative record of what changed and why.

In a secure software lifecycle, this same capability supports integrity, traceability, reproducibility, and auditability: teams can connect a change request to the affected requirements, source code, build, test evidence, and release configuration. These records help ensure that the implemented project scope remains consistent with approved decisions and that changes do not introduce unmanaged risk. PMI describes configuration management as an important project-management practice for controlling product and project artifacts; see the PMBOK Guide resources. NIST also details the role of configuration management in maintaining the integrity of system components in SP 800-128.

QUESTION NO: 16

What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

A. Determine software product or service requirements.

B. Develop software requirements.

C. Implement change control procedures.

D. Develop evaluation criteria and evaluation plan.

E. Create acquisition strategy.

ANSWER: A B D E

Explanation:

The planning phase of a Software Assurance (SwA) acquisition establishes what is being acquired, the assurance expectations that apply, and the method by which prospective suppliers and their products will be assessed. **Determine software product or service requirements** is foundational because acquisition planning must define the needed capability, security expectations, operational environment, and applicable constraints before a supplier can be selected. **Develop software requirements** converts those needs into sufficiently specific acquisition requirements, including security and assurance-related requirements that can be included in solicitation and contract materials.

Create acquisition strategy defines the approach for obtaining the product or service and for incorporating software-assurance considerations throughout supplier selection and contract execution. **Develop evaluation criteria and evaluation plan** ensures that the acquisition team has documented, repeatable criteria for evaluating supplier proposals, evidence, and assurance capabilities against the established requirements. These planning activities support risk-informed supply-chain and software-acquisition decisions, consistent with NIST guidance on integrating cybersecurity supply-chain risk management into acquisition processes. See NIST SP 800-161 Rev. 1 and ISC2's CSSLP Certification Exam Outline.

QUESTION NO: 17

Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Cryptographer

B. Cryptography

C. Kerberos

D. Cryptanalysis

ANSWER: D

Explanation:

Cryptanalysis is correct because it is the discipline of examining cryptographic systems to identify weaknesses and use them to recover protected information, such as plaintext from ciphertext or, in some circumstances, the secret key. It encompasses analysis of an algorithm's mathematical properties, its implementation, its protocol use, and operational factors that may expose information. Successful cryptanalysis does not necessarily require guessing a key by brute force; it can exploit weaknesses in the cryptographic design, errors in implementation, insecure key handling, or information leaked through observable behavior. In secure software development, understanding cryptanalysis helps teams select well-vetted algorithms and configurations, avoid designing proprietary cryptography, protect key material, and recognize that a cryptographic control must be implemented and used correctly to provide its intended protection. NIST describes cryptanalysis as the study of mathematical techniques for attempting to defeat cryptographic techniques, while its cryptographic standards and guidance support the use of approved, publicly analyzed mechanisms. See the NIST Cryptanalysis glossary definition and NIST Cryptographic Standards and Guidelines.

QUESTION NO: 18

John works as a systems engineer for BlueWell Inc. He has modified the software, and wants to retest the application to ensure that bugs have been fixed or not. Which of the following tests should John use to accomplish the task?

A. Reliability test

B. Functional test

C. Performance test

D. Regression test

ANSWER: D

Explanation:

Regression test is correct because it is performed after software has been changed to confirm that previously identified defects have been corrected and that the change has not unintentionally damaged behavior that worked before. John has modified the application and needs to retest it, which is the core scenario for regression testing. A regression test suite typically re-executes relevant existing test cases, including tests for the repaired defect and tests covering related functions, interfaces, data handling, and critical user workflows. This provides evidence that the fix works in the updated build while preserving the integrity of established functionality.

Within a secure software lifecycle, regression testing is particularly important because code modifications—even apparently small fixes—can introduce unexpected side effects, reopen prior defects, or alter security-relevant behavior. Teams commonly automate repeatable regression tests and run them as part of continuous integration so that changes are validated consistently before release. The ISTQB glossary defines regression testing as testing of a previously tested program following modification to ensure defects have not been introduced or uncovered in unchanged areas. See the ISTQB regression testing glossary entry and NIST's Secure Software Development Framework.

QUESTION NO: 19

Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?

A. Gray-box testing

B. White-box testing

C. Black-box testing

D. Unit testing

ANSWER: A C

Explanation:

Black-box testing is appropriate because it evaluates the network from an external, attacker-like perspective without relying on detailed prior knowledge of its architecture, hosts, configurations, or trust relationships. Maria can use discovery, enumeration, and controlled vulnerability assessment techniques to identify exposed services, accessible systems, and security weaknesses as they would be observed by an unauthorized party. This perspective is valuable for establishing the organization's externally visible attack surface.

Gray-box testing is also appropriate for a newly appointed network administrator conducting an authorized security assessment. As she gains limited organizational access—such as approved credentials, network ranges, diagrams, or selected configuration details—she can use that partial knowledge to test realistic insider or authenticated attack paths. Combining limited internal knowledge with adversarial testing helps assess weaknesses that are not visible from outside the environment, including authorization boundaries, segmentation, and exposed administrative services. The ISC2 CSSLP examination outline includes security testing as a secure software lifecycle competency, while OWASP's testing guidance describes information-gathering and testing activities that support both external and knowledge-assisted assessments. See the ISC2 CSSLP Certification Exam Outline and the OWASP Web Security Testing Guide.

QUESTION NO: 20

In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?

A. Public cloud

B. Community cloud

C. Private cloud

D. Hybrid cloud

ANSWER: C

Explanation:

Private cloud is correct because its infrastructure is provisioned for exclusive use by a single organization. That organization may own, manage, and operate the environment itself, or those responsibilities may be performed by a third party. A private cloud can also be located on the organization's premises or hosted off premises; exclusivity of use by one organization, rather than physical location or ownership, is the defining characteristic. This model enables an organization to apply cloud characteristics—such as on-demand resource provisioning, elasticity, and pooled resources—within a more controlled environment aligned to its specific security, governance, compliance, and operational requirements. NIST's cloud-computing definition identifies private cloud as infrastructure provisioned for exclusive use by a single organization comprising multiple consumers, and notes that it may be owned, managed, and operated by the organization, a third party, or a combination of both. See NIST SP 800-145, The NIST Definition of Cloud Computing. For ISC2 CSSLP preparation, understanding the deployment model helps practitioners identify the governance boundaries and responsibility arrangements relevant to secure software deployment and operation. See the ISC2 CSSLP Exam Outline.

QUESTION NO: 21

You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?

A. NIST Special Publication 800-53

B. NIST Special Publication 800-59

C. NIST Special Publication 800-53A

D. NIST Special Publication 800-37

ANSWER: C

Explanation:

NIST Special Publication 800-53A is the appropriate guide because it defines assessment procedures for determining whether security and privacy controls have been implemented correctly, are operating as intended, and are producing the desired outcome for federal information systems and organizations. It operationalizes control assessment by providing a structured methodology, including assessment objectives and potential methods such as examination, interviewing, and testing. A security engineer can use these procedures to collect evidence, assess control effectiveness, document findings, and support ongoing authorization and risk-management activities.

The publication is designed to be used with the control catalog in NIST Special Publication 800-53, but its specific purpose is assessment rather than control selection. This distinction is important: verifying effectiveness requires repeatable assessment procedures and evidence-based evaluation criteria. NIST describes SP 800-53A as the guide for assessing security and privacy controls in information systems and organizations. The current publication is available from the NIST SP 800-53A Rev. 5 publication page. Its role also aligns with the assessment and monitoring activities within the NIST Risk Management Framework, where organizations evaluate controls to make informed risk and authorization decisions.

QUESTION NO: 22

Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?

A. Management review

B. Code review

C. Peer review

D. Software audit review

ANSWER: B C

Explanation:

Code review is the direct security-focused examination of source code or code changes to find and remediate implementation defects before release. Reviewers can trace how input is handled, validate bounds checking and memory management, identify unsafe formatting operations, examine concurrent access to shared resources, and confirm that errors and allocated resources are handled safely. This makes code review particularly effective for the listed vulnerability classes, which commonly arise from programming and design choices that may not be visible through high-level project reporting or compliance activities.

Peer review is also correct because code review is commonly conducted as a peer review: one or more technically qualified colleagues examine a developer's code and provide feedback or approval. A structured peer-review practice provides independent scrutiny of changes, helps apply secure coding standards consistently, and promotes correction of defects before they reach production. The OWASP Code Review Guide describes source-code review as a method for identifying security vulnerabilities, while NIST's Secure Software Development Framework calls for reviewing code and addressing identified vulnerabilities as part of secure development practices. See the OWASP Code Review Guide and NIST SP 800-218, Secure Software Development Framework.

QUESTION NO: 23

Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

A. National Security Agency (NSA)

B. National Institute of Standards and Technology (NIST)

C. United States Congress

D. Committee on National Security Systems (CNSS)

E. U.S. Department of Commerce (through NIST)

ANSWER: B E

Explanation:

The National Institute of Standards and Technology (NIST) is the federal agency whose statutory and operational role most directly matches this objective. NIST develops measurement science, reference materials, technical standards, and related technologies that support reliable commerce, industrial innovation, interoperability, and public well-being. Its published mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. This language closely reflects the purpose described in the question. NIST performs this work through research laboratories, calibration and measurement services, cybersecurity publications, and standards-related collaboration with industry and other government bodies. See NIST's official About NIST page and its statutory authorities in 15 U.S.C. § 272.

The U.S. Department of Commerce is also correctly included because NIST is an agency within that department. Accordingly, the department carries out this measurement, standards, and technology mission through NIST as one of its constituent agencies. In a multiple-choice context where more than one answer is required, both the specific operating agency and its parent federal department appropriately identify the responsible federal organization.

QUESTION NO: 24

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

A. DDoS attack

B. Evasion attack

C. Insertion attack

D. Dictionary attack

E. A FIN-flood distributed denial-of-service attack

ANSWER: A E

Explanation:

The described event is a distributed denial-of-service attack, specifically a TCP FIN-flooding form of resource-exhaustion attack. A distributed denial-of-service attack uses many compromised hosts under an attacker's control to send traffic or protocol packets toward one target. The defining detail is the coordinated use of multiple compromised computers, which makes the activity distributed rather than a single-source denial-of-service event. Hundreds of FIN packets can consume processing capacity, connection-state resources, network bandwidth, or the resources of intervening security devices, particularly when source addresses are spoofed. Source spoofing also makes source-based filtering and attribution more difficult and can contribute to the attack's effectiveness. This scenario is therefore properly classified as a denial-of-service condition caused by a distributed set of attack systems. The closely related wording "A FIN-flood distributed denial-of-service attack" identifies the same correct classification more specifically: FIN packets are the mechanism, while distributed denial of service is the attack category. NIST describes denial-of-service attacks as attempts to prevent or impair authorized use of systems, networks, or applications and identifies distributed forms as involving multiple sources. See NIST's denial-of-service attack glossary entry and CISA's overview of denial-of-service attacks.

QUESTION NO: 25

You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?

A. Performance test

B. Functional test

C. Reliability test

D. Regression test

ANSWER: B

Explanation:

Functional test is correct because functional testing verifies that implemented software behavior conforms to specified functional requirements, including the handling of required data and the production of expected outputs. In this scenario, the relevant outputs are the application's displays and reports. A functional test exercises the build using defined inputs and data conditions, then confirms that the resulting screens, calculations, workflows, and report content match the documented expected results. This provides direct evidence that the build delivers the capabilities required by its specification and that data is processed and presented correctly to users.

For secure software lifecycle work, this verification should be based on traceable acceptance criteria and test cases derived from documented requirements. Expected displays and report results should be explicit, reproducible assertions so that the test produces objective evidence suitable for release decisions and regression coverage in later builds. Requirements-based testing is a core quality practice because it demonstrates that software functionality has been implemented as intended. See the NIST Guide to Software Testing and the OWASP Web Security Testing Guide for testing guidance and the role of repeatable, requirements-informed verification activities.

QUESTION NO: 26 - (SIMULATION)

SIMULATION

Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

ANSWER: See the explanation for the answer

Explanation:

Answer: `technical effort`

A **technical effort** is any activity that affects defining, designing, building, or executing/implementing a task, requirement, or procedure. It is part of technical management used to move from a business need through system deployment and operation.

QUESTION NO: 27

In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management

B. Exception management

C. Configuration Management

D. Change Management

E. Incident Management

ANSWER: B E

Explanation:

Exception management is the primary process described because it addresses deviations from an expected business-process flow. Exceptions can arise when input is malformed, a required process step cannot be completed, an external dependency fails, or an infrastructure or network condition prevents normal processing. Effective exception management combines automated detection, logging, routing, and correlation with intervention by qualified personnel who can diagnose the underlying condition, correct data or processing failures, and ensure that the process is brought to an appropriate resolution. This operational capability is particularly important in secure software lifecycles because unhandled exceptions may affect availability, data integrity, auditability, and the reliability of business transactions.

Incident Management is also applicable when the deviation manifests as an operational service issue, especially an infrastructure, application, or connectivity failure. Its purpose is to restore normal service operation as quickly as possible while documenting, categorizing, escalating, and coordinating resolution of the incident. In practice, exception-management tooling may detect and create records for failures that service-management personnel then manage as incidents. This connection supports timely containment and recovery while preserving evidence needed for follow-up analysis. See the ITIL incident management overview and NIST's Computer Security Incident Handling Guide.

QUESTION NO: 28

Fill in the blank with an appropriate security type. applies the internal security policies of the software applications when they are deployed.

A. Programmatic security

ANSWER: A

Explanation:

Programmatic security is the appropriate completion because it enforces application security through logic implemented in the software itself. The application code makes security-relevant decisions at runtime, such as determining whether an authenticated user has the required role to invoke an operation or perform a particular business task. This allows security behavior to reflect the application's business context, including the current user, the requested action, and the resources involved. When the application is deployed, these internally implemented controls operate as part of the deployed software and govern access according to the security logic built into the code. In secure software development, this approach requires developers to apply authorization checks consistently and to ensure that security decisions cannot be bypassed through alternate application flows. The Java EE security guidance describes programmatic security as security implemented by application code, including methods used to check caller roles and control access during execution. See the Oracle Java EE Tutorial: Securing Enterprise Beans and the OWASP Authorization Cheat Sheet for guidance on implementing and validating authorization controls.

QUESTION NO: 29

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

A. DoD 8910.1

B. DoD 7950.1-M

C. DoDD 8000.1

D. DoD 5200.22-M

E. DoD 5200.1-R

ANSWER: B

Explanation:

DoD 7950.1-M is the correct designation for the *Defense Automation Resources Management Manual* (DARMM). This manual established Department of Defense policy and procedural guidance for managing automation resources, a term used at the time for information-technology capabilities, systems, and associated resources. The "-M" suffix identifies the issuance as a manual, which aligns with the title named in the question. DARMM addressed management disciplines relevant to the planning, acquisition, operation, control, and use of automated information resources across the Department of Defense. Although this is a historical issuance and the DoD's information-management policy framework has since evolved, the document number and title remain the recognized pairing for questions concerning legacy DoD automation-resource governance. The Defense Technical Information Center maintains catalog information for the historical publication at DTIC's record for the Defense Automation Resources Management Manual. Current and historical DoD issuance-management information is available through the DoD Issuances website.

QUESTION NO: 30

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III

B. MAC IV

C. MAC I

D. MAC II

ANSWER: D

Explanation:

MAC II is correct because the Mission Assurance Category construct in DoD 8500.2 classified systems according to the required integrity and availability of the mission information they process, store, or transmit. A MAC II system supports missions for which unauthorized modification, destruction, or loss of information could seriously impair mission performance; it therefore requires *high integrity*. Its services must remain available to support the mission, but the effect of a disruption does not rise to the highest availability requirement, so it is assigned *medium availability*. This pairing—high integrity and medium availability—is the defining assurance profile for MAC II and drives selection of applicable information-assurance controls under the legacy DoD 8500.2 framework. Although DoD 8500.2 has since been superseded as DoD cybersecurity policy evolved toward the Risk Management Framework, recognizing its MAC definitions remains useful when interpreting legacy system documentation, control baselines, and examination scenarios. The historical instruction is available through the Defense Technical Information Center copy of DoD 8500.2. For current DoD cybersecurity governance and RMF implementation context, consult DoD Manual 8500.01.

QUESTION NO: 31

Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42

B. NIST SP 800-53A

C. NIST SP 800-60

D. NIST SP 800-53

E. NIST SP 800-37

F. NIST SP 800-59

G. NIST SP 800-115

ANSWER: A G

Explanation:

NIST SP 800-42 is directly correct because its official title is *Guideline on Network Security Testing*. It was published by NIST to help organizations plan and conduct network security testing, including the use of testing techniques to identify vulnerabilities and verify the security posture of networked systems. Its guidance addresses planning, executing, and analyzing technical network tests within an organized security-testing process. The publication remains the NIST document that most precisely matches the wording of the question. See the official publication record at NIST SP 800-42.

NIST SP 800-115 is also correct as a current, broader NIST technical guide for information-security testing and assessment. It provides practical methodology for planning and conducting technical assessments, including network discovery, network vulnerability scanning, and penetration testing. These activities are central forms of network security testing, so this publication also provides applicable NIST guidance for such testing. Its guidance emphasizes defining assessment objectives and scope, selecting suitable techniques, conducting tests in a controlled manner, analyzing findings, and reporting results so that discovered weaknesses can be remediated effectively. The official NIST publication page is available at NIST SP 800-115.

QUESTION NO: 32

You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. Qualitative risk analysis uses accurate and unbiased data to produce credible probability and impact assessments.

B. A qualitative risk analysis encourages biased data to reveal risk tolerance

C. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.

D. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.

E. A qualitative risk analysis requires fast and simple data to complete the analysis.

ANSWER: A D

Explanation:

Qualitative risk analysis depends on credible information to assign relative probability and impact ratings consistently. Therefore, the data used for the analysis must be accurate and unbiased. Accurate data means that the ratings are supported by the best available facts, estimates, assumptions, and expert input regarding each identified risk. Unbiased data means that the assessment is not distorted by personal preferences, organizational politics, optimism, pessimism, or an attempt to force a desired project outcome.

The statement "A qualitative risk analysis requires accurate and unbiased data if it is to be credible" expresses this requirement directly. The restored statement, "Qualitative risk analysis uses accurate and unbiased data to produce credible probability and impact assessments," conveys the same valid principle and completes the otherwise blank option. Credible qualitative assessments allow the project team to prioritize risks appropriately, focus response-planning effort on the most significant exposures, and communicate risk information reliably to stakeholders. PMI describes qualitative risk analysis as a process for prioritizing individual project risks for further analysis or action by assessing their probability of occurrence and impact; this prioritization is only dependable when its underlying information is sound. See PMI's PMBOK Guide and Standards and the PMI Lexicon of Project Management Terms.

QUESTION NO: 33

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. Information systems acquisition, development, and maintenance

C. DC Security Design & Configuration

D. EC Enclave and Computing Environment

ANSWER: A C D

Explanation:

DoD Instruction 8500.2 organized its Information Assurance controls into eight IA areas. "VI Vulnerability and Incident Management" is one of those areas and covers controls intended to identify, assess, remediate, and manage vulnerabilities and security incidents. "DC Security Design & Configuration" is also an IA area, encompassing security engineering, system design, configuration, and related technical control considerations. "EC Enclave and Computing Environment" is another defined area and addresses protections implemented within the computing environment and enclave architecture. These names are part of the historical IA-control structure in DoDI 8500.2, alongside Identification and Authentication, Enclave Boundary Defense, Physical and Environmental, Personnel, and Continuity. Although DoDI 8500.2 has since been cancelled and replaced as DoD policy evolved toward the Risk Management Framework, its IA-area terminology is the applicable basis for this question. The archived instruction can be consulted at DoD Instruction 8500.2. For the current overarching DoD cybersecurity policy framework, see DoD Instruction 8500.01.

QUESTION NO: 34

Which of the following authentication methods is used to access public areas of a Web site?

A. Anonymous authentication

B. Biometrics authentication

C. Mutual authentication

D. Multi-factor authentication

ANSWER: A

Explanation:

Anonymous authentication is the appropriate method for providing access to publicly available areas of a website. It permits a visitor to request and receive designated public content without supplying individual credentials, such as a username, password, certificate, or biometric factor. In a web-server implementation, the server commonly maps unauthenticated requests to a restricted service or guest identity. That identity must be granted only the minimum permissions required to read the intended public resources, following least-privilege principles. This approach allows websites to publish pages, images, documents, and other content intended for general visitors while retaining authentication requirements for administrative functions, personal data, transactions, and protected application areas. The term “anonymous” describes the visitor’s experience: the visitor does not establish a personally authenticated session merely to view the public content. It does not eliminate the need for secure server configuration, authorization controls, logging, transport protection where appropriate, or careful separation of public and restricted resources. Microsoft’s IIS documentation describes Anonymous Authentication as allowing users to access content without being prompted for credentials: IIS Anonymous Authentication. NIST’s digital identity guidance also distinguishes unauthenticated public access from authentication used to establish a claimant’s identity: NIST SP 800-63-3.

QUESTION NO: 35

Della work as a project manager for BlueWell Inc. A threat with a dollar value of $250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

A. $2,000

B. $2,500

C. $3,510

D. $3,500

E. $250,000 × 0.01 = $2,500

ANSWER: B E

Explanation:

The annualized loss expectancy is **$2,500**. Annualized loss expectancy is a quantitative risk measure that estimates the monetary loss an organization expects from a specific threat over one year. It is calculated by multiplying the single loss expectancy by the annual rate of occurrence: **ALE = SLE × ARO**. In this scenario, the stated dollar value of $250,000 is the single loss expectancy, meaning the loss expected from one occurrence of the threat. The frequency of 0.01 per year is the annual rate of occurrence, representing an expected occurrence rate of one event per 100 years. The calculation is therefore $250,000 × 0.01, which equals $2,500. The option expressing this calculation, **$250,000 × 0.01 = $2,500**, is mathematically equivalent to **$2,500** and is also correct. This use of expected loss and event frequency supports risk analysis decisions, including evaluating whether a proposed control is financially justified. NIST defines annualized loss expectancy as an estimate of expected loss over a year in its Cybersecurity Glossary; see also NIST’s Guide for Conducting Risk Assessments.

QUESTION NO: 36

Which of the following elements sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security)?

A. User data constraint

B. Authorization constraint

C. Web resource collection

D. Accounting constraint

ANSWER: A

Explanation:

User data constraint is correct because it defines the transport-protection requirement for requests covered by a web application security constraint. In a servlet deployment descriptor, this is represented by the `<user-data-constraint>` element and its `<transport-guarantee>` setting. A transport guarantee of `CONFIDENTIAL` requires the container to ensure that requests are transmitted over a connection that protects confidentiality, normally HTTPS using TLS. This protects data in transit between the client and server, including sensitive request content such as credentials, session identifiers, and submitted form data. The related `INTEGRAL` value expresses an integrity-protection requirement, while `NONE` does not require protected transport. When the configured transport guarantee requires confidentiality and a client requests a constrained resource without the required protection, the servlet container is responsible for directing the client to an appropriate secure connection. This control concerns the security of the communication channel itself and is therefore the servlet security-constraint element that establishes TLS-protected access for covered requests. The Jakarta Servlet specification describes user-data constraints and transport guarantees in its security-constraint section: Jakarta Servlet Specification. Oracle's Java EE tutorial also documents the use of transport guarantees for secure web application communication: Securing Web Applications.

QUESTION NO: 37

A security architect wants to prevent a compromised web server from directly connecting to the organization's payment-processing database. Which of the following architectural controls most directly supports this objective?

A. Network segmentation

B. Data compression

C. Code obfuscation

D. Data encryption

ANSWER: A

Explanation:

Network segmentation is correct because it separates systems into distinct network zones and restricts communications between them through controlled enforcement points. In this scenario, the web server can be placed in a presentation-tier zone while the payment database is placed in a protected data-tier zone. Firewall or security-group rules can then permit only required application-tier communication and deny direct web-server access to the database.

Network segmentation reduces lateral movement and limits the consequences of a compromised component, but it must be combined with secure application design, strong authentication, least privilege, monitoring, and properly configured access rules. Encryption protects data confidentiality in transit or at rest, but it does not by itself prevent an authorized network connection from being established. NIST describes boundary protections as controls that monitor and control communications at external and key internal boundaries. See NIST SP 800-53 Rev. 5, SC-7.

QUESTION NO: 38

Which of the following attacks causes software to fail and prevents the intended users from accessing software?

A. Enabling attack

B. Reconnaissance attack

C. Sabotage attack

D. Disclosure attack

ANSWER: C

Explanation:

Sabotage attack is correct because it targets the availability and proper operation of a software system. Its purpose is to disrupt, damage, disable, or otherwise interfere with the application or the resources on which it depends, so legitimate users cannot use the software as intended. In practice, sabotage can include intentionally corrupting application components or data, disabling required services, deleting critical resources, or exhausting a system's capacity until it can no longer provide its expected function. The resulting condition is a denial of service: the system may be unavailable entirely, may fail unpredictably, or may be unable to serve authorized users within required operational parameters. Availability is a core security objective and includes ensuring timely, reliable access to information and systems for authorized users. This description directly matches the effect stated in the question: software failure combined with prevention of intended-user access. The CSSLP examination outline includes availability-related secure software concerns within its coverage of application security concepts and software lifecycle activities. See the ISC2 CSSLP Exam Outline and NIST's definition of availability.

QUESTION NO: 39

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

A. Phase 2

B. Phase 4

C. Phase 1

D. Phase 3

ANSWER: D

Explanation:

Phase 3 is correct because it is the Validation phase of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Its purpose is to validate that the prior lifecycle and certification activities have resulted in an information system that operates as intended within its specified computing environment. This validation provides the evidence needed to confirm that the system's security posture, implemented controls, configuration, and operational environment are consistent with the established accreditation basis and acceptable residual-risk decision.

DITSCAP was a predecessor DoD certification-and-accreditation approach and is now primarily encountered in legacy material; its concepts were later superseded by the DoD Risk Management Framework. Nevertheless, the phase terminology remains important when interpreting older DoD security lifecycle documentation. NIST describes DITSCAP as a standard management process for certifying and accrediting DoD information technology systems in its DITSCAP glossary entry. For historical context on the transition from DITSCAP-related certification and accreditation practices to the RMF, see NIST SP 800-37 Rev. 1.

QUESTION NO: 40

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

A. System Definition

B. Validation

C. Identification

D. Accreditation

E. Verification

F. Re-Accreditation

G. Initiate and Plan Certification and Accreditation (C&A)

H. Implement and Validate Assigned Information Assurance Controls

I. Make Accreditation Decision

J. Maintain Authorization to Operate

K. Decommission

ANSWER: G H I J K

Explanation:

The DIACAP lifecycle was organized around five formal activities: *Initiate and Plan C&A*, *Implement and Validate Assigned IA Controls*, *Make Accreditation Decision*, *Maintain Authorization to Operate*, and *Decommission*. These activities establish a continuous process for defining the system and certification effort, applying and assessing assigned information-assurance controls, documenting the authorizing official's accreditation decision, sustaining the approved security posture during operation, and securely retiring the system. Therefore, the newly added answers use the official DIACAP activity names and collectively represent the complete DIACAP process.

The terminology in the question's supplied explanation appears to conflate DIACAP with the older DITSCAP model. DIACAP superseded DITSCAP and used the five activities listed here rather than a four-phase System Definition/Verification/Validation/Re-Accreditation structure. DIACAP was later replaced across DoD by the Risk Management Framework, but its historical process terminology remains relevant when answering legacy certification questions. DoD's current RMF policy and lifecycle context are available in DoDI 8510.01, Risk Management Framework for DoD Systems; NIST also describes the authorization lifecycle and ongoing security-management concepts in NIST SP 800-37 Rev. 2.

QUESTION NO: 41

FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact?

A. The loss of confidentiality, integrity, or availability might result in major damage to organizational assets.

B. The loss of confidentiality, integrity, or availability might result in severe or catastrophic harm, including serious life-threatening injuries or loss of life.

C. The loss of confidentiality, integrity, or availability might result in major financial loss.

D. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent that the organization is unable to perform one or more of its primary functions.

ANSWER: A B C D

Explanation:

Under FIPS 199, a high-impact security objective applies when the loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic adverse effect* on organizational operations, organizational assets, or individuals. The listed effects accurately reflect the consequences identified for that impact level. Major damage to organizational assets and major financial loss are expressly included as potential severe consequences. Severe harm to individuals can include serious, life-threatening injuries or loss of life. A high impact can also involve severe degradation in, or loss of, mission capability to the extent that the organization cannot perform one or more of its primary functions. These criteria are applied independently to confidentiality, integrity, and availability when determining the security categorization of an information type or information system. FIPS 199 therefore supports selecting every listed consequence as a valid high-level potential impact effect. See NIST FIPS 199 and the supporting security-categorization guidance in NIST SP 800-60 Volume I.

QUESTION NO: 42

Which of the following roles is also known as the accreditor?

A. Data owner

B. Chief Risk Officer

C. Chief Information Officer

D. Designated Approving Authority

ANSWER: D

Explanation:

Designated Approving Authority is the role traditionally known as the accreditor. In legacy U.S. federal information assurance terminology, accreditation was the formal management decision to authorize a system to operate based on an assessment of its security controls and the acceptance of residual risk. The Designated Approving Authority held the authority to make that risk-based authorization decision on behalf of the organization. This role is accountable for determining whether the system's security posture, documented risks, and planned safeguards are acceptable for the system's intended mission or business use. Modern NIST Risk Management Framework terminology generally uses *Authorizing Official* instead of Designated Approving Authority and refers to the decision as *authorization*, rather than accreditation. The underlying governance responsibility remains the same: a senior official accepts responsibility for operating a system at a defined level of risk. NIST SP 800-37 defines the Authorizing Official as the senior official who accepts security and privacy risk to organizational operations and assets, individuals, other organizations, and the nation. See NIST SP 800-37 Rev. 2 and the NIST glossary definition of Designated Approving Authority.

QUESTION NO: 43

ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.

A. Inter-Organization Co-operation

B. Information Security Risk Treatment

C. CSFs (Critical success factors)

D. System requirements for certification bodies management

E. Terms and Definitions

F. Guidance on process approach

ANSWER: C

Explanation:

CSFs (Critical success factors) is correct. ISO/IEC 27003 provides implementation guidance for an information security management system (ISMS), supporting organizations as they establish, implement, maintain, and continually improve an ISMS aligned with ISO/IEC 27001. Critical success factors are an important implementation concept because they identify the organizational conditions needed for an ISMS initiative to succeed. These conditions include visible management commitment, adequate resources, defined responsibilities, appropriate awareness and competence, effective communication, and integration of information-security objectives with business objectives. Identifying CSFs helps an implementation team focus on the practical enablers that make ISMS processes sustainable rather than treating implementation as only a documentation exercise. The ISO/IEC 27003:2010 edition used the critical-success-factor terminology reflected in this question, while the current edition continues to provide ISMS implementation guidance. ISO's catalogue describes ISO/IEC 27003 as guidance for implementing an ISMS: ISO/IEC 27003:2010. The current publication record is available at ISO/IEC 27003:2017.

QUESTION NO: 44

Which of the following techniques is used to identify attacks originating from a botnet?

A. Passive OS fingerprinting

B. Recipient filtering

C. IFilter

D. BPF-based filter

ANSWER: A

Explanation:

Passive OS fingerprinting is the correct technique. It identifies characteristics of an endpoint's operating system by observing network traffic rather than actively probing the endpoint. In particular, implementations can inspect TCP connection behavior, including fields and options associated with SYN and SYN-ACK packets, and compare the observed characteristics with known operating-system signatures. This information gives defenders useful context for traffic sources and targets involved in suspicious activity.

For botnet-related investigation, passive fingerprinting can support detection and triage by revealing groups of hosts that display consistent or unexpected network-stack characteristics, associating observed operating systems with source IP addresses, and enriching intrusion-detection alerts. Security monitoring systems can use that context when correlating command-and-control behavior, scanning, distributed attacks, or other anomalous traffic that may be generated by compromised hosts. Because it is passive, the technique can be deployed to observe production traffic without sending packets that might affect systems or alert an attacker. The approach is therefore particularly useful as network telemetry that improves attribution, relevance scoring, and investigation of suspected botnet activity. The underlying TCP behavior used for fingerprinting is defined in RFC 793, and a practical passive-fingerprinting implementation is documented by the p0f project.

QUESTION NO: 45

Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

A. Provide Ongoing Skills and Knowledge

B. Verify and Validate Security

C. Manage Project Risk

D. Improve Organization's System Engineering Process

ANSWER: A C D

Explanation:

The SSE-CMM groups its process areas into broad categories so that security engineering work is supported by disciplined project management and organizational capabilities. *Provide Ongoing Skills and Knowledge* is a Project and Organizational Practice because an organization must establish and sustain the security-engineering competencies, training, and knowledge needed to perform its work effectively. *Manage Project Risk* belongs in this category because identifying, evaluating, treating, and monitoring risks is a continuing management activity that enables the technical effort to remain aligned with security, cost, schedule, and mission objectives. *Improve Organization's System Engineering Process* is also included because organizational process improvement institutionalizes lessons learned and strengthens the engineering process used across projects. These are specifically identified among the SSE-CMM Project and Organizational Practice process areas, alongside activities such as quality assurance, configuration management, project planning and control, supplier coordination, and support-environment management. The model's purpose is to provide a capability-based framework for assessing and improving systems security engineering processes, including both technical engineering practices and the organizational practices that enable them. See the Software Engineering Institute's SSE-CMM Model Description Document and NIST's SSE-CMM glossary entry.

QUESTION NO: 46

What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

A. Risk analysis plan

B. Staffing management plan

C. Risk management plan

D. Human resource management plan

E. Risk management plan that defines the quantitative risk-analysis methodology

ANSWER: C E

Explanation:

The **Risk management plan** is the governing component of the overall project management plan for risk-related work, including quantitative risk analysis. It defines the methodology, roles and responsibilities, funding, timing, risk categories, probability and impact definitions, reporting formats, and tracking approach used to manage project risk. These planning decisions establish how quantitative techniques—such as expected monetary value analysis, sensitivity analysis, simulation, or decision-tree analysis—will be selected, performed, documented, and used to support project decisions.

A matrix environment may affect responsibility assignments, escalation paths, resource availability, and stakeholder coordination, but it does not change the fact that the risk management plan directs the project's risk-management processes. The added wording, **Risk management plan that defines the quantitative risk-analysis methodology**, identifies the same authoritative planning artifact more specifically and is therefore also correct. PMI describes project risk management as including planning risk management and performing quantitative risk analysis, with the risk management plan providing the framework for those activities. See PMI's Practice Standard for Project Risk Management and the PMBOK Guide and Standards.